**Test Script #5 - Summary:**

This script will test security functions and security administration of the system. The "system" is defined as all of the components necessary to provide the clinical functionality tested in the clinical scenarios, as described in the Application for Certification. This system consists of all necessary network nodes, all platform components delivered by the Applicant, and all the Applicant components (e.g. documentation) included with the system.

| **Test Script #5 - Security** |
|---|
| **Protecting the Privacy of Health Information**<br>This test will verify that the product being tested meets basic security and reliability requirements as listed in applicable County criteria that:<br>Adhere to Privacy and Security Best Practices;<br>Can be tested as part of clinical or administrative process scenarios; and<br>Are readily measureable or observable |

| **Test Script #5 - Assumptions** |
|---|
| In relation to defining the scope of the system to be tested, Applicants may assign certain functionality to a third party (e.g. when security and operating functions are handled by the operating system, a third party component, tool, or service). Where a function is indicated as “assignable”, Applicants can indicate they are assigning. In this case, they must provide related materials for self-attestation.<br><br>For example, for backup and restore: Applicants that use a third party database utility could assign backup functionally and provide related documentation for self-attestation.<br><br>This test scenario starts with a pre-existing “security administrative” user. This user needs to have all permissions necessary to carry out security administrative tasks and has no rights to access clinical data. This does not imply that a product couldn’t provide a more complex security administrative permissions system.<br><br>This scenario requires the creation of one ***Clinical User*** . The Applicant can choose the name for this ***Clinical User*** . |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.01 | Generate a backup copy of the application data, security credentials and log/audit files. | A full backup is created.<br>If R1 is assigned, see step 7.01. | | ❑ Pass | ❑ Fail |
| 5.02 | If the system claims to be available 24x7, verify that the system has the ability to run a backup concurrently with the operation of the application. | Backup runs concurrently with the application.<br>If R3 is assigned, see step 7.02. | | ❑ Pass | ❑ Fail |
| 5.03 | Restore whole system from backup. | Restoration results in a fully operational and secure state, including restoration of:<br>• Application data<br>• Security credentials<br>• Log/audit files<br>If R2 is assigned, see step 7.03. | | ❑ Pass | ❑ Fail |
| | **Establish User Accounts** | | | | |
| 5.04 | Login as Security Administrator. | Login successful | | | |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.05 | Access the directory of users. | System maintains a directory of all clinical personnel who use or access the system. | | ❑ Pass | ❑ Fail |
| 5.06 | Review user attributes required to determine the system security level to be granted to each user. | System maintains a directory that stores the attributes. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.07 | Create one valid ***Clinical User*** account as per the documentation provided during self-attestation step 6.13. | User account successfully created as per documentation provided during self-attestation. Appropriate privileges are assigned.<br>If S23 is assigned, see step 7.04. | | ❑ Pass | ❑ Fail |
| 5.08 | Assign clinical rights to the user created in step 5.07. This user account will have no administrative rights but will have clinical rights. | Appropriate privileges are assigned. | | ❑ Pass | ❑ Fail |
| 5.09 | Access the directory of users. | Directory of clinical personnel is as in step 5.05 above, and updated with addition of user created in step 5.07. | | ❑ Pass | ❑ Fail |
| 5.10 | Show identifiers required for licensed clinicians to support the practice of medicine. | At a minimum, the system shall maintain a directory of state medical license, DEA, NPI and UPIN number. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.11 | Show directory of clinical personnel external to the organization who are not users of the system. Applicant can use example provided in set up data, or other data as exists. | System maintains a directory of clinical personnel external to the organization who are not users of the system to facilitate communication and information exchange | | ❑ Pass | ❑ Fail |
| 5.12 | Set password strength rules to require 8 characters minimum. | Password strength rules are set to 8 characters minimum.<br>If S13 is assigned, see step 7.05. | s-02 2004, | ❑ Pass | ❑ Fail |
| 5.13 | Set authentication failure lockout parameters to 3. | Authentication failure lockout value set to 3 (for purposes of this test).<br>If S15 is assigned, see step 7.06. | | ❑ Pass | ❑ Fail |
| | **Test access controls** | | | | |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.14 | Access Protected Health Information (PHI).<br>PHI means the information as defined by the Centers for Medicare and Medicaid Services (CMS). | Access denied. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.15 | Access security audit trails. | Access provided | | ❑ Pass | ❑ Fail |
| 5.16 | Logout as Security Administrator. | Logout successful | | | |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.17 | Login as **Clinical User** created in this scenario. Enter password with wrong case. Applicant could use Notepad to enter passwords, and cut and paste into login screen, or enter using an onscreen keyboard. | Login denied.<br>If S20 is assigned, see step 7.07. | | ❑ Pass | ❑ Fail |
| 5.18 | Verify that the login failure result given to the user does not include any hints as to the reason for the failure. | User should be aware that authentication failed, but receive no further information (e.g. doesn't state the reason by advising incorrect user ID, incorrect password, incorrect case, etc.)<br>A message that includes a reminder about Caps Lock is acceptable.<br>If S17 is assigned, see step 7.08. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.19 | Login as Clinical User created in this scenario using the correct username and password.<br>Applicant could use Notepad to enter passwords, and cut and paste into login screen, or enter using an onscreen keyboard. | Login successful.<br>If S12 is assigned, see step 7.09.<br>If S20 is assigned, see step 7.07.<br><br>In any case, this step must be demonstrated to evaluate compliance with S2 and S3 even if S12 and S20 are assigned. | | ❑ Pass | ❑ Fail |
| 5.20 | Verify that the login procedure did not show the password in readable form. | Password was not displayed during entry.<br>If S26 is assigned, see step 7.10.<br>If S17 is assigned, see step 7.08. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.21 | Access security audit trails. | Access denied | | ❑ Pass | ❑ Fail |
| 5.22 | Logout as ***Clinical User.*** | Logout successful | | | |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.23 | Login as ***Clinical User*** created in this scenario; use different case in username. | Login successful.<br>If S12 is assigned, see step 7.09.<br>If S18 is assigned, see step 7.11.<br>If S20 is assigned, see step 7.07. | | ❑ Pass | ❑ Fail |
| 5.24 | Access patient record for Jennifer Thompson. | Access successful. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| | **Test authentication system**<br>**Have the Security Administrator set session inactivity to 1 minute and then change it immediately following the next step to test S 14, and then resume normal operation so the test script is not interrupted by session inactivity timeouts.** | | | | |
| 5.25 | Allow session inactivity to exceed 1 minute. Attempt to access patient record for Jennifer Thompson. | Session lockout activated. Access denied.<br>If S14 is assigned, see step 7.12. | | ❑ Pass | ❑ Fail |
| 5.26 | Re-authenticate into session. Attempt to access patient record for Jennifer Thompson. | Authentication is required before access to patient record is allowed.<br>If S12 is assigned, see step 7.09.<br>If S14 is assigned, see step 7.12. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.27 | Prior to this step, have the Security Administrator set the password strength requirement to disallow passwords with only letters.<br>Change password to one with all letters. | User cannot change password to all letters because of enforcement of password strength rules as documented.<br>If S19 is assigned, see step 7.13. | | ❑ Pass | ❑ Fail |
| 5.28 | Logout as ***Clinical User.*** | Logout successful. | | | |
| 5.29 | Login as ***Clinical User*** ; use an invalid password. Attempt to login in with invalid password 3 times. | Login denied 3 times.<br>If S15 is assigned, see step 7.06. | | ❑ Pass | ❑ Fail |
| 5.30 | Login as ***Clinical User*** ; use the valid password. | Login denied (due to previous invalid attempts at limit).<br>If S15 is assigned, see step 7.06. | | ❑ Pass | ❑ Fail |
| 5.31 | Login as Security Administrator.<br>Unlock clinical user account. | Login successful.<br>Clinical user account unlocked. | | | |
| 5.32 | Logout as Security Administrator. | Logout successful. | | | |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.33 | Login as ***Clinical User*** ; use the valid password. | Login successful. | | | |
| 5.34 | Logout as ***Clinical User*** . | Logout successful. | | | |
| 5.35 | Login as Security Administrator. | | | | |
| 5.36 | Modify Clinical User account to remove, suspend, or terminate user privileges, without removing or deleting the user account.<br>Access the directory of users. Review Clinical User account attributes to determine that the Clinical User still exists, and that its privileges are suspended [i.e., have been removed, suspended, or terminated]. | Clinical User account remains in the user directory, but its privileges are appropriately removed, suspended, or terminated. | | ❑ Pass | ❑ Fail |
| 5.37 | Logout as Security Administrator. | | | | |
| 5.38 | Login as ***Clinical User*** . | Login denied. | | | |
| 5.39 | Verify that the login failure result does not include any hints as to the reason for the failure. | User should be aware that authentication failed, but receive no further information (e.g. doesn't advise user privileges are removed, suspended, or terminated, etc.) | | ❑ Pass | ❑ Fail |
| 5.40 | Login as Security Administrator. | | | | |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.41 | Access **Clinical User** account. Modify **Clinical User** account to restore user privileges. | Access successful. Modification successful. | | ❑ Pass | ❑ Fail |
| | Logout as Security Administrator. | | | | |
| 5.42 | Login as ***Clinical User*** . | Login successful. | | ❑ Pass | ❑ Fail |
| 5.43 | Access chart for Jennifer Thompson. | Access allowed to Jennifer Thompson's chart. | | ❑ Pass | ❑ Fail |
| 5.44 | Logout as ***Clinical User*** . | Logout successful. | | | |
| | **Access control testing** | | | | |
| 5.45 | Login as Security Administrator. | Login successful | | | |
| 5.46 | Reset password for ***Clinical User*** . | Clinical User's password is reset.<br>If S16.1 is assigned, see step 7.15. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.47 | View audit trail configuration to assess ability to enable or disable auditing for event or group of related events. | System allows security administrator to enable or disable tracking of system events or groups of events. | | ❑ Pass | ❑ Fail |
| 5.48 | View all audit events recorded in Appendix D that were recorded as an auditable event by the Proctor throughout Scenarios 1-5. | Events identified as noted in earlier steps. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.49 | For all audit events recorded in Appendix D that were recorded as an auditable event by the Proctor throughout Scenarios 1-5, verify the audit log contains the following information:<br>• Date and time of event<br>• Where the event occurred (e.g. software component, hardware component, or the IP address of the client device initiating the event or, if the event originated on the server, the IP address of the server)<br>• Type of event<br>• Subject identity (patient id, user id)<br>• The outcome | Audit log for all the audited events requested in Appendix D contains the appropriate information. | | ❑ Pass | ❑ Fail |
| 5.50 | Access audit record generated in step 5.48. | The time of audit record is in the exact ISO 8601 format. Example: "1994-11-05T08:15:30-05:00" corresponds to November 5, 1994, 8:15:30 am, US Eastern Standard Time. | | ❑ Pass | ❑ Fail |

| Test Step | | Expected Result | Actual Result | Pass/Fail | |
|---|---|---|---|---|---|
| 5.51 | Logout Security Administrator. | Logout successful. | | | |
| 5.52 | Login as the ***Clinical User*** whose password was reset. | Login successful. The system will prompt the Clinical User to change the password. If S16.2 is assigned, see step 7.16. | | ❑ Pass | ❑ Fail |